



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,908	05/16/2005	Bernd Meycr	30691/DP018	6775
4743 7590 04/27/2007 MARSHALL, GERSTEIN & BORUN LLP 233 S. WACKER DRIVE, SUITE 6300 SEARS TOWER CHICAGO, IL 60606			EXAMINER DOAN, TRANG T	
			ART UNIT	PAPER NUMBER
			2131	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		04/27/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/506,908	MEYER ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Trang Doan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 07 February 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 February 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
- ☒ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

**DETAILED ACTION**

1. This action is in response to the amendment filed on 02/07/2007.
2. The new drawings have been entered.
3. The 112, 2<sup>nd</sup>, paragraph rejection has been withdrawn.
4. Claims 1-2, 4-9, 12-17, 19, 21 and 23 are amended; Claims 1-24 are pending in this application.

***Response to Arguments***

5. Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejection's set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-15 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowney et al. (US 5987140) (hereinafter Row) in view of Toh et al. (Pub. No. 2002/0129238) (hereinafter Toh).
8. Regarding claim 1, Row discloses the steps of generating key information in a contact station; forming encrypted checking information from the key information and from the transaction indicator in the contact station (Row: see figure 4 and column 13

lines 4-20: Merchant generates a random encryption key and then uses the random encryption key to encrypt combined block (530: comprises authorization request, public key certificate, signature public key certificate and digital signature) to form encrypted combined block (550)), encrypting the key information in the contact station (Row: column 13 lines 21-24), transmitting the encrypted checking information and the encrypted key information to an intermediate station (Row: column 13 lines 29-36), storing the encrypted key information and the encrypted checking information in the intermediate station and subsequently transmitting the encrypted key information and the encrypted checking information to a cryptographic module at a different time from the transfer between the contact station and the intermediate station (Row: see figure 1C). Row does not explicitly disclose temporarily storing the encrypted information (i.e., encrypted key information, encrypted checking information) in the intermediate station. Toh discloses temporarily storing the encrypted information (i.e., encrypted key information, encrypted checking information) in the intermediate station (Toh: see figures 3 and 5; paragraphs [0013, 0094, 0096]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of temporarily storing the encrypted information in the intermediate station (i.e., operations center) of Toh within the system of Row because there is a need for a flexible delivery system which provides integrated key management so that reliable delivery and end-to-end security can be achieved, thus providing some or all of the following benefits: (1) reliable/guaranteed delivery for transactions-a delivery will not be lost; (2) confidentiality for transactions-only the recipient can open a delivery; (3) non-repudiation for transactions; and (4) complex

routing of transactions among multiple recipients, including over the Internet between different organizations (Toh: paragraph [0018]).

9. Regarding claim 2, Row in view of Toh discloses randomly generating the key information (Row: column 13 lines 4-14).

10. Regarding claim 3, Row in view of Toh discloses configuring at least one of the encrypted key information and the encrypted checking information is in such a way that it cannot be decrypted in the intermediate station (Row: column 16 lines 10-22).

11. Regarding claim 4, Row in view of Toh discloses decrypting the encrypted key information with a key contained in the cryptographic module (Row: column 13 lines 45-58).

12. Regarding claim 5, Row in view of Toh discloses entering document data into the cryptographic module (Row: column 14 lines 1-13).

13. Regarding claim 6, Row in view of Toh discloses irreversibly linking the document data to the key information (Row: see figures 6 A and B).

14. Regarding claim 7, Row in view of Toh discloses irreversibly linking the document data and the key information by forming a check value from the key information (Row: column 12 lines 43-65).

15. Regarding claim 8, Row in view of Toh discloses combining the document data and the key information that is irreversibly linked to the document data for form at least one of a document and a data record and transmitting the document or data record to a checking station (Row: see figures 6 A and B).

16. Regarding claim 9, Row in view of Toh discloses wherein the document or data record transmitted to the checking station is transmitted at least partially in plain text (Row: see figures 6 A and B).

17. Regarding claim 10, Row in view of Toh discloses entering the encrypted checking information into the document or data record that is transmitted to the checking station (Row: see figures 6 A and B).

18. Regarding claim 11, Row in view of Toh discloses encrypting information remaining in the cryptographic module in such a way that it can be decrypted in the cryptographic module (Row: see figure 8).

19. Regarding claim 12, Row in view of Toh discloses supplying the cryptographic module with the information from a cryptographically reliable station that can be relied on by the checking station (Row: see figure 12 and column 17 lines 44-67 and column 18 lines 1-33).

20. Regarding claim 13, Row in view of Toh discloses using cryptographic encryptions that the checking station can reverse (Row: column 13 lines 4-13).

21. Regarding claim 14, Row in view of Toh discloses supplying the cryptographic module via communication partners that are cryptographically non-reliable and forwarding information to the cryptographic module at a different point in time from the transfer of information between the contact station and the intermediate station (Row: see figure 1C and column 18 lines 34-42).

22. Regarding claim 15, Row in view of Toh discloses supplying of the cryptographic module via communication partners that are cryptographically not reliable is carried out

in such a way that an exchange of information within a dialog is not necessary (Row: see figure 1B).

23. Regarding claim 23, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

24. Regarding claim 24, Row in view of Toh discloses wherein the information is encrypted in such a way that it cannot be decrypted in the value transfer center (Row: column 16 lines 10-22).

25. Claims 16-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Row in view of Toh, and further in view of Singer (US 6724894) (hereinafter Singer).

26. Regarding claim 16, Row in view of Toh does not explicitly disclose cryptographically linking the key information and the encrypted checking information to each other, such that said linking cannot be discovered by means of crypto-analysis. Singer discloses cryptographically linking the two types of data to each other, such that said linking cannot be discovered by means of crypto-analysis (Singer: see Abstract and column 3 lines 45-62). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of crypto-analysis of Singer to Row in view of Toh's method to reduce side channel attacks pose a significant threat to cryptographic system. Differential power analysis attacks allow an attacker to extract secret protected information from a supposedly secure cryptographic device by measuring variations in power consumption over time, and then applying sophisticated analysis to this information (Singer: column 1 lines 33-36).

27. Regarding claim 17, Row in view of Tod in view of Singer discloses wherein the cryptographic linking of the key information and the encrypted checking information is such that non-linear fractions are added that are known only to the reliable contact station and to the checking station (Row: see figure 6 A and B).

28. Regarding claim 18, Row in view of Toh does not explicitly disclose wherein the generated forgery-proof documents or data records contain monetary value information. Singer discloses wherein the generated forgery-proof documents or data records contain monetary value information (Singer: column 3 lines 7-25). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of encrypted postage value of Singer to Row in view of Toh's method to generate secure postal indicia by selected data on the mailpiece as the postage value and then uses a secret key to encrypt the postage value to form an encrypted postage value.

29. Regarding claim 19, Row in view of Toh does not explicitly disclose connecting the monetary value information to the document or data record, and forming a check value by comparing the monetary value information to the document or data record. Singer discloses connecting the monetary value information to the document or data record in such a way that a check value can be formed by comparing the monetary value information to the document or data record (Singer: column 7 lines 43-49). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of hash value of Singer to Row in view of Toh's method to create a check value (or hash value) based upon the monetary value to verify that the monetary value



has not been altered because altering the monetary value would change the check value (or the hash value).

30. Regarding claim 20, Row in view of Toh does not explicitly disclose wherein the monetary value information contains proof of the payment of postage amounts. Singer discloses wherein the monetary value information contains proof of the payment of postage amounts (Singer: column 9 lines 5-9 and column 10 lines 3-19 and column 3 lines 7-25). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of hash value of Singer to Row in view of Toh's method to create a check value (or hash value) based upon the monetary value to verify that the monetary value has not been altered because altering the monetary value would change the check value (or the hash value).

31. Regarding claim 21, Row in view of Toh does not explicitly disclose linking the monetary value information to identification data. Singer discloses linking the monetary value information that proves the payment of postage amounts to identification data of the document producer (Singer: column 4 lines 23-43). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of hash value of Singer to Row in view of Toh's method to create a check value (or hash value) based upon the monetary value to verify that the monetary value has not been altered because altering the monetary value would change the check value (or the hash value).

32. Regarding claim 22, Row in view of Toh does not explicitly disclose linking the monetary value information to address data. Singer discloses linking the monetary value information to address data (Singer: column 4 lines 44-65). Therefore, it would

have been obvious to one ordinary skill in the art to apply the teaching of linking the postage value to address data of Singer to Row in view of Toh's method depending on the verification strategy additional elements, including delivery address information, may be included. An indicium should, at a minimum, contain: 1) the security data, and 2) the digital token produced by an encryption of the security data. Cryptographic authentication proves integrity of these elements (Singer: column 4 lines 37-43).

### ***Conclusion***

33. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Trang Doan  
Examiner  
Art Unit 2131

T.D.

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100